DCI

The Director of Central Intelligence

Washington, D.C. 20505

1 May 1981

Stanley Sporkin, Esquire
Securities and Exchange Commission
500 North Capitol Street, N.W.
Washington, D.C. 20549

Dear Stanley:

This is an area in which I would like to see your imagination and resourcefulness. Take a look at these papers and I will talk to you when I see you.

Yours,

Bill

William J. Casey

Enclosures:
Various news clippings
re technology

SAN JOSE NEWS
5 March 1981

Silicon Valley spying

By Pete Carey
Staff Writer

The Soviet Union is lagging behind the Silicon Valley's electronic technology and bent on catching up — any way it can.

The Soviets buy the valley's best ideas on the open market whenever possible. When they can't obtain the technology legally, recent federal investigations show, they deal with companies that export it illegally.

During an investigation in Southern California, eight agents of the KGB, the Soviet version of the CIA, were photographed taking delivery of highly sensitive military equipment.

FBI Director William H. Webster said recently that the KGB has been active in the Bay Area for 10 years, during which time Silicon Valley has become the world's leading research and development center for solid state electronics.

In a talk to the Commonwealth Club in San Francisco, Webster warned that "certain foreign intelligence operations have been specifically assigned to steal this technology. Educate your employees who don't think this sort of thing exists. This is important for the self-interest of the company — and for our national well-being."

Investigators are probing a network of foreign agents and businesses who have helped unfriendly nations avoid U.S. embargos on the export of technology.

The Customs and Commerce departments stepped up investigation and prosecution of such cases last year. In September, a "working group" was formed of several federal agencies to deal with export violations.

A pattern has emerged of American and foreign businessmen buying technology, exporting it to neutral countries such as Switzerland and Austria, and then transshipping it into the Soviet Union.

A current case involves Continental Technology Corp. of Torrance. Run by two people, a West German and a Russian who became a naturalized U.S. citizen, Continental is suspected of buying advanced electronics technology from contractors in Santa Clara County and sending it to the Soviet Union. No charges have been filed but the case is before a federal grand jury.

Cases resolved in the past year:

✓ A Belgian citizen, Marc Andre DeGeyter, was jailed after search warrants showed his firm was shipping a secret Intel Corp. computer chip to the Soviet Union. Search warrants in the case showed DeGeyter's company, Computer Engineering and Services Accounting, Brussels, had a contract with Techgmashimport, a Soviet international trading company.

✓ Walter J. Spawr, president of Spawr Optical Research, Inc., Corona, was found guilty of shipping laser mirrors that could be used on satellites to the Soviet Union via a Switzerland export "drop." Spawr received a five-year sentence, with all but six months suspended, and the company was fined $100,000.

✓ Otto Poeschl, a West German trading as Arga Warenhandelgesellschaft and Tewifa Investment Corp., was denied export privileges for 10 years after he was found sending illegally purchased computer parts and memory cores to Warsaw Pact nations. The cover destinations were in Austria.

✓ A Montreal and a Tel Aviv company — DeVimy Test Lab Ltd. and Excel Industries — were denied export privileges after sending computer equipment to the Soviet bloc through a complex network of "cover" routes. Shipments would go to Amsterdam and other intermediate points from which they were sent to Vienna. From there, the material was shipped into the Soviet Union.

✓ A South African, Joan P. Taylor of Taylor Enterprises, was caught illegally routing $205,000 worth of arms from Olin-Winchester Corp. to South Africa with phony export destinations. She was barred from exporting from the United States for 10 years.

Underground channels

In Silicon Valley, underground channels sometimes take advantage of thieves to obtain material, according to one authority.

"It's similar to what the valley has with parts being stolen for their gold," said John Shea, a San Jose technical consultant to defense and intelligence agencies.

Shea, whose Technology Analysis Group analyzes Soviet electronics equipment for various government agencies, put together a "Soviet shopping list" for the Mercury News.

The list, Shea says, should include locally manufactured high-speed microprocessors used in missiles; radiation-hardened circuitry; circuits that can store video signals; and the latest technologies in manufacturing the dense, high-speed integrated circuits that have made Silicon Valley famous.

Also on the list are advanced techniques for making microcircuitry such as complimentary metal oxide semiconductors and silicon-on-sapphire methods.

"They are trying to pick up on the latest high technology in integrated circuit areas," Shea said.

"Responsible government sources report concern within the Department of Defense that France may be inadvertently or consciously making significant high technology available to the Soviets either in commercial or para-military products," he said.

Shea said the French recently showed an interest in high-speed computer applications to military-aerospace systems and electro-mechanical technology.

'Prime target'

"When you couple these two technologies, you get applications in electronic countermeasures, electronic warfare and communications and reconnaisance satellites.

"You can be sure that Silicon Valley is a prime target for overt and covert intelligence-gathering," Shea said.

On the other hand, he noted that U.S. manufacturers with overseas distribution outlets can make it easy for unfriendly nations to acquire commercially available products.

Often, he said, "The Russians can buy what they want outside the United States."

CONTINUED

Two recent developments indicate the Soviet Union is about three years behind the United States in solid state technology.

'A good copy'

First, the CIA obtained a Russian microprocessor from a missile captured by the Israelis. It is a copy of the 8080 microprocessor, introduced by Intel Corp. in 1977. The 8080 has been superceded by more advanced Intel microprocessors.

The Soviet version of the 8080 is a much larger chip than Intel's, but remains what sources described as "a good copy" of the device.

The second development came when the Carter administration froze an export license, preventing Control Data Corp. from selling an advanced computer to the Soviet news agency Tass. The Carter administration said the computer contained too high a level of vital technology.

In response, the Soviet Union sent one of its own integrated circuits to the United States to show they already had the technology.

Analysts say the Soviet-made chip is a copy of a Mostek Corp. microprocessor. It has more liberal timing and voltage parameters, which increases the yield and simplicity of manufacturing, but it is a good copy, sources say.

During a rare spot check of high technology leaving the country last year, the Customs Department in Long Beach turned up 28 major violations in three weeks.

The violations ranged from mislabelling packing crates and exporting without a license to shipments by suspected "front companies" diverting U.S. technology to unfriendly nations.

Seven companies are being investigated as the result. The suspect exports included, among other things, aircraft design material valued at $5 million; two $250,000 shipments of machine guns and silencers; a $400,000 shipment of computer parts and a large shipment of space satellite systems.

"Three weeks of spot checks will keep us busy for six months of investigation," said Ken Ingleby, special agent in charge of Customs' Terminal Island office in Los Angeles.

Problem laws

Another investigator said that "the laws are a problem. They (exporters) don't have to file on shipments which leave the country by ship until five days after the ship sails. They can file then, saying it's anything — jellybeans, washing machine parts or whatever. How are we going to check?"

Although stolen circuitry apparently is not the primary source of advanced American technology for unfriendly nations, investigators suspect it is a factor.

"All our information indicates that some of these (stolen or counterfeit) devices are ending up in the Soviet Union," reports Wayne Brown, a Santa Clara County sheriff's deputy who investigates electronics thefts.

Police are looking at a recent $64,000 loss reported by Advanced Micro Devices Corp. to the Sunnyvale Department of Public Safety.

AMD is missing some of its most advanced circuits, which sell for $36 to $50 apiece. The circuits are capable of storing video-encoded information.

AMD declined comment.

Doug Southard, who prosecutes electronics cases for the district attorney's office, says, "We want to break this thing up because it's hurting the economy of this area and it has possible international implications as well."

ARTICLE APPEARED ON PAGE 128
BUSINESS WEEK
27 April 1981

How Russia snares high-technology secrets

A key element of America's post-Afghanistan sanctions against the Soviet Union—the sweeping ban on virtually all U. S. high-technology exports—has not only failed to influence the Kremlin but may even be backfiring. Moscow is making more illicit deals that circumvent international trade controls, as well as taking greater advantage of the legal loopholes that exist abroad.

As a result, the Reagan Administration will soon push the Western allies to put more muscle behind their restrictions on Soviet trade. The immediate goal is to stem the flow of semiconductor and computer technology, much of which has military potential.

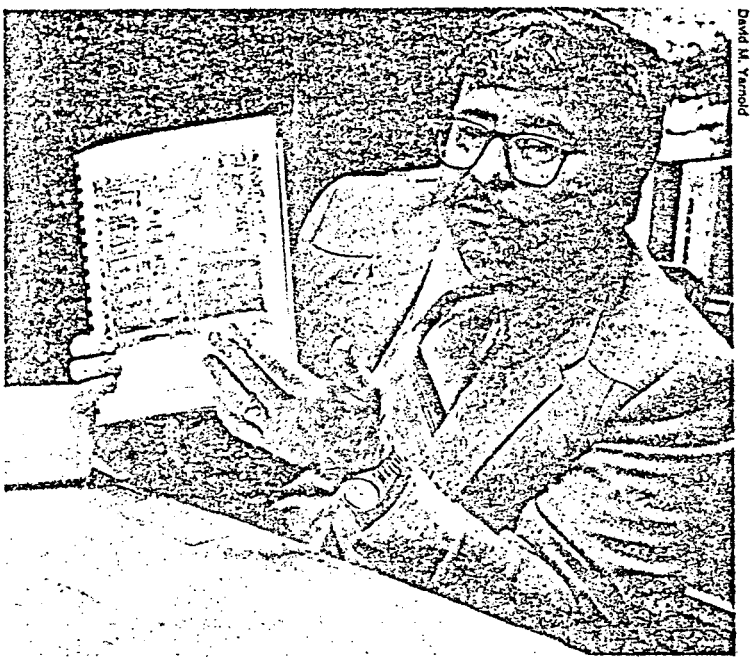
Longer term, many members of the Reagan camp, including Secretary of State Alexander M. Haig Jr., are calling for a tightening of trade policy. They believe the Western allies must mobilize their economic strength to put effective pressure on the Soviets. "We need to seriously consider developing, in concert with our allies, the capability to wage limited economic war against the Soviet Union," says one ranking Reaganite.

The organization for such an undertaking already exists in the Coordinating Committee on Export Controls. Cocom was formed during the cold war era to help contain Soviet expansionism by restricting trade. It has compiled a foot-thick list of products that cannot be exported to Communist countries without first obtaining a license. After Afghanistan, President Carter never asked the other Western allies to emulate his blanket embargo on high-technology goods, but the Cocom nations—the members of the North Atlantic Treaty Organization, minus Iceland, plus Japan—did agree to grant no more licenses for listed products destined for Russia.

U. S. chip and computer skills leak via illicit deals and legal loopholes

Given the economic plight of Western Europe, there is scant chance of a general accord that would significantly reduce trade with the Soviet bloc, so the Reagan Administration will insist on strict enforcement of Cocom guidelines. A U. S. trade official notes that many Cocom members "have been reluctant partners, at best." And since the U. S. imposed its embargo, he adds, some Cocom governments—notably France—have encouraged their domestic companies to grab business from U. S. companies.

Many U. S. businessmen are confused by Washington policy. Although the blanket embargo was lifted a year ago, U. S. business continues to be penalized by Washington's overzealous enforcement of Cocom rules. Other nations thus are often wrongly blamed for ignoring the rules. Sometimes the rules are bent, but most countries strictly control shipments of strategic items.



David M. Yarnold

Defense consultant Shea and chip-circuit diagram: The foe is gaining.

To the Reagan Administration, though, the issue is more fundamental than whether specific rules are bent or broken. Reagan's advisers want the Cocom countries to formulate a consistent policy to replace the ad hoc, shoot-from-the-hip approach that characterized the Carter team. The Reaganites believe that the inconsistency of their predecessors sapped the cohesion of Cocom.

Disintegration. "I don't know at what point Cocom began to disintegrate, but I concede that it has," says Lawrence J. Brady, the new Assistant Secretary of Commerce-designate for trade. Brady is an avowed critic of high-technology sales to the Soviets, and his appointment is a clear signal that the U. S. position is hardening. "Multinational controls can be made to work," adds Brady, "if we sit down with our allies and determine where we are going."

But putting effective controls on technology transfer has never been easy. In an age of handheld microcomputers and a host of consumer products containing little bits of silicon that can provide intelligence experts with important clues about technological progress, it may be impossible. Security at many small semiconductor producers—or users—is often rather lax, says a U. S. Customs Service inspector in Europe. And once a Soviet agent has stolen samples or bribed an employee to do so, notes a European intelligence specialist, "you can easily take 20,000 semiconductors out in a diplomatic suitcase." Sources in Washington say that the KGB has 30 agents in California's Silicon Valley, plus others in Phoenix and Dallas—all charged with obtaining data on microelectronics technology.

Once the Kremlin obtains a semiconductor chip, the Soviets are adept at "reverse engineering"—industry jargon for shaving the chip down by hair-thin layers and photographing the circuitry exposed in the process. This yields a three-dimensional schematic of the microcircuits. Control Data Corp. late last year obtained a Soviet-made microprocessor and, after reverse engineering and analysis, the Minneapolis computer maker estimates that Russia's semiconductor technology lags behind that of the U. S. by only about three years.

Long lags. In practice, says John D. Shea, president of Technology Analysis Group Inc., a consultant for the Defense Dept., Soviet spies might do better in Macy's or some other department store. Shea asserts that the Soviets can learn more about semiconductor technology by buying commercial products than by stealing defense data. By the time the Pentagon nails down specifications for a new chip, calls for bids, and gives a contract to the lowest bidder, the semiconductor companies are turning out the next generation of chips for commercial applications. "The microelectronic devices in toys, automobiles, appliances, and industrial tools are more sophisti-

CONTINUED

cated than th[illegible]es in our weapons and satellites," Sh[illegible] maintains.

According to a position paper just published by the Computer & Business Equipment Manufacturers Assn., a trade organization, the government's methods of controlling technology transfer have not adjusted to this accelerating rate of change in the technological content of commercial products. The paper also argues that the U. S. embargo had no chance of succeeding because what the Soviets cannot obtain from U. S. companies can almost invariably be purchased elsewhere.

'Front' companies score. Smuggling in a suitcase, or simply buying in a store

Many trade experts doubt that illicit shipments have even unofficial sanction of Cocom governments. Instead, they hold that businessmen, especially small businessmen in both Europe and the U. S., are the culprits—and are more willing to risk violating export controls during economic slumps. "Then the profit motive supersedes the sense of patriotism," sighs a federal official. Philip R. Bowen, regional director of investigations for the U. S. Customs Service in San Francisco, points out that unlicensed exports of embargoed goods increased significantly during the 1975 recession, and the same thing seems to be happening now. Allegations of export-control violations in the U. S. climbed last year to 350, up from 200 in 1979.

Violations. Bowen says that since 1976 his office has handled about 25 cases involving high-technology violations, and he expects perhaps 10 more this year. Recent examples include:

- Continental Technology Corp., a Torrance (Calif.) company jointly run by a West German and a naturalized-U. S. citizen born in Russia, is suspected of buying about $15 million worth of advanced electronics equipment and laundering it through 11 front companies to the Communist bloc. The case is before a Los Angeles grand jury.
- Two executives of Quest Electronics, a Santa Clara (Calif.) electronics distributor, were arrested last October and charged with conspiring to export illegally some $10,000 worth of computer-circuit chips stolen from Intel Corp.
- Last January, Walter J. Spawr, president of Spawr Optical Research Inc., in Corona, Calif., and his wife were convicted of shipping mirrors for high-energy lasers to the Soviet Union by way of Switzerland. The mirrors sold to Moscow were identical to those purchased by the U. S. Air Force Weapons Laboratory.

The company was fined $100,000, but the Spawrs are appealing. During the appeal process, notes Theodore W. Wu, assistant U. S. att[illegible], they remain immune from restrict[illegible]s: "There is nothing to keep them from doing it again."

Pressure. Small companies can be easy prey for KGB agents. One common tactic is for a Russian agent to set up a local business as a front and begin buying nonsensitive products from a supplier of, say, equipment for making semiconductor chips. Gradually, the agent increases his purchases until the point where the Kremlin indirectly accounts for a substantial portion of the vendor's sales. Then the agent uses that leverage to persuade the supplier to sell the export-controlled equipment, and the equipment is diverted to a "drop" in Austria or such non-Cocom countries as Liechtenstein, Switzerland, or Sweden. From there, it is reexported to one or more countries, ultimately ending up in Russia. A trade expert in Scandinavia notes that Finland is another funnel for a lot of high-tech goods, "but you'll never find it in their export statistics—unless you happen to notice the unusual volume of shipments to such places as Swaziland."

"Canada is an excellent location for front companies," says a Customs Service official, "because it's the only country where you don't need an export license, if the shipment is for use in Canada." The Reagan Administration is considering various methods to crack down on such practices. One proposal is to raise the reward for information leading to the conviction of violators from the current $50,000 to $250,000.

Troubling ties. James Brewster, a London consultant on Soviet trade, points to a "very strong French presence" in the Soviet Union since the Carter embargo. Shea of TAG is clearly troubled by the close ties between the two countries. He points out that Harris Corp., a Florida-based company, and France's Matra have formed a joint venture, Matra-Harris, to design and produce semiconductors in France—and, in April, Matra-Harris got another partner, Intel Corp., a California company that has pioneered microprocessor technology. What worries Shea is that Harris is among the leading producers of semiconductors that are resistant to radiation damage. "This is leading-edge technology with massive military applications," says Shea, adding that his U. S. intelligence contacts figure that once the French get their hands on this knowhow, the Soviets will field it in military systems within two or three years.

As a result, Shea asserts that it is "very probable" that all joint-venture agreements involving high-technology transfer and any foreign company will in the future require federal approval. Key personnel at Defense and Commerce want such deals to be reviewed just as if they involved military hardware. ■

NEWSWEEK
12 November 1979

NATIONAL AFFAIRS

SPYING ON U.S. BUSINESS

As in most real-life espionage stories, the details are hazy even now. But sometime in the early 1970s, U.S. intelligence officials say, a train carrying an IBM 370 computer sold to Poland by a European firm mysteriously broke down along the border between Poland and the Soviet Union. When the train began rolling again, the computer was no longer aboard. In March 1973, officials say, Soviet authorities contacted a European computer firm to buy spare parts for an IBM 370. The parts were available, they were told, but the firm needed to know the serial number of the computer. Sure enough, the serial number turned out to be that of the missing IBM 370—then among the most sophisticated computers in the world.

The computer's apparent diversion into Russian hands is an extreme case—but in many less dramatic ways, U.S. officials believe, the Soviet Union is stepping up its attempts to steal U.S. military and technological secrets by penetrating American industry. "We can lock up everything in the Pentagon," says FBI chief William Webster, "but the same information may be in a safe in a company building" where it is "much more vulnerable." Safeguarding those secrets is a gargantuan task: some 11,000 firms have access to classified defense information, and about 120,000 of their employees have top-secret clearances. Both the FBI and the Central Intelligence Agency intensified security checks of industrial firms—but CIA director Stansfield Turner termed the CIA's findings "discouraging." Soviet snoops are assumed to monitor communications at major defense plants, and last February six Boeing Co. employees lost their security clearances because they carelessly sent information about the MX missile over an ordinary phone line.

BRIBES: The Soviet-bloc countries employ a wide range of techniques to crib American technological innovations. FBI agents in Chicago, for example, are investigating a case in which the Polish Government apparently set up a dummy corporation to acquire industrial data that had been embargoed for export to Communist countries. And a Reston, Va., computer firm told the FBI in September that one of its executives had been offered a $500,000 bribe by a Soviet agent for a copy of an unclassified bit of software used to program the computers of a number of major corporations, including Gulf Oil and Citibank. Companies in financial trouble are special targets for foreign agents, who offer much-needed contracts, then demand help in circumventing U.S. export regulations. "The implications of the strings attached may not be obvious at first," an FBI official says. "Nevertheless, the businessman is slowly drawn into a foreign intelligence network."

Knowledgeable spies can reap a rich harvest of advanced technical data without resorting to skulduggery. The Soviets, for example, subscribe to a biweekly report on current scientific research published by the government-run National Technical Information Service. It collates only unclassified research, but some of the papers provide valuable technical clues—"a running account of the level of U.S. technology on a very, very timely basis," says one U.S. expert. The Soviet Union has a standing request to receive microfilm copies of all documents relating to such fields as "missile technology" and "optics and lasers." Inevitably, a document or two turns out to have been improperly declassified.

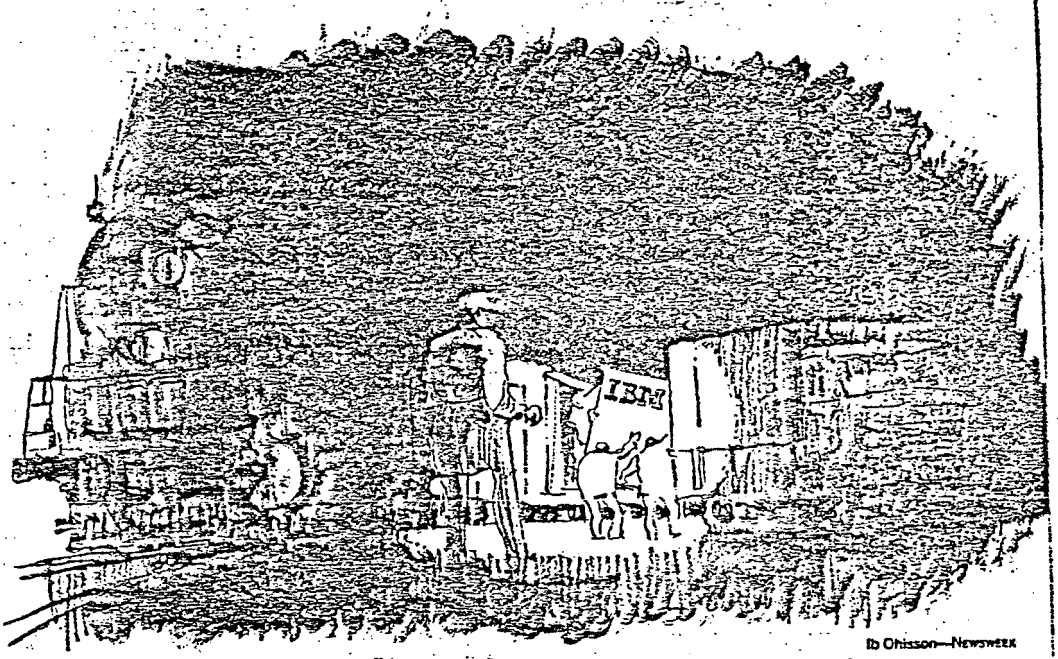
Similarly, participants in scientific meetings that routinely include Soviet experts often seem "lax . . . about the protection of militarily significant technologies," complains J. Fred Bucy, president of Texas Instruments. And Webster is concerned by the influx of visiting scientists and businessmen from the Communist bloc. One Hungarian physicist was allowed to study magnetic-bubble memories for computers—until a defector revealed the Hungarian had a deadline for delivering a prototype to Moscow.

Controlling the spread of sophisticated American technology becomes more difficult when scientific breakthroughs enter commercial production, as they have in computers, microelectronics, fiber optics and lasers. Federal export regulations restrict the sale of products that could be of military value to the Soviet bloc—but the rules can be difficult to apply, forcing case-by-case evaluations. "We will license [the export of] computers of a certain size," says a U.S. Commerce Department official. "But we will absolutely not license . . . the technology to produce them." Some American firms dodge the regulations in order to make a sale. Last month, two former executives of I.I. Industries pleaded guilty to the illegal sale of semiconductor-manufacturing equipment worth $300,000 to East Germany. Similar sales by other firms could total as much as $35 million.

EQUIPMENT: The Soviet espionage campaign now aims to copy both the product and the manufacturing process. The CIA has found, for example, that the microcircuitry inside a Soviet electronic calculator duplicated that of an American-made model—a relatively simple bit of "reverse engineering." But U.S. experts were disturbed that the Soviets had also obtained advanced American-made equipment to manufacture the microcircuits, probably through a legal sale to Yugoslavia.

Stemming the steady leakage of American technology poses a series of policy dilemmas for U.S. officials. It is one thing to crack down on espionage or illegal sales. But many American advances are there for the asking. Sophisticated technology is America's most competitive export on the world market, and the free exchange of technical information is highly valued by scientists. The Soviet bloc's access to scientific research can be eliminated only by suppressing scientific debate and business enterprise—and so far no one seems willing to go that far.

TOM MORGANTHAU with DAVID C. MARTIN and ELAINE SHANNON in Washington



Ib Ohlsson—Newsweek

An IBM 370 disappears in Poland: Stepped-up efforts to steal U.S. technological secrets

ARTICLE APPEARED
ON PAGE A 1

THE WALL STREET JOURNAL
28 April 1981

The Silicon Spies

Semiconductor Firms Are Plagued by Thefts Of 'Hi-Tech' Materials

Federal, State Lawmen Say Soviet Bloc Is Getting Many Illegal Shipments

Intel Corp. Plugs a Leak

By MARILYN CHASE and JIM DRINKHALL
Staff Reporters of THE WALL STREET JOURNAL

SUNNYVALE, Calif.—It looked like a simple larceny when $64,000 of semiconductor chips disappeared from Advanced Micro Devices Inc.—an increasingly common occurrence here in the technology-rich "Silicon Valley."

"Somebody just walked in off the street and took the parts right out of inventory," says W.J. Sanders, the president of the company. "It was embarrassing."

What gives a sinister dimension to the heist is that the stolen circuits had been designed to military specifications for use in the nation's missile and aerospace programs. Where these chips are now is a $64,000 question. The fear is that they'll turn up in somebody else's missiles, possibly the Russians'. It wouldn't be the first time.

Says Assistant U.S. Attorney Theodore Wu, who is conducting a federal grand-jury investigation in Los Angeles of technological espionage, "The Silicon Valley and Southern California are the cradles of the illegal and clandestine shipment of strategic goods to the Soviet Bloc." In San Jose, in the heart of the "valley," the Santa Clara County sheriff's office is conducting its own investigation of the disappearance of sophisticated electronics equipment.

A Race With the Soviets

Thefts and diversion of electronic components have occurred at such major producers as Intel Corp., Texas Instruments Inc. and National Semiconductor Corp. as well as many smaller companies. The cost of thefts to Silicon Valley companies alone is running about $20 million a year, industry sources say.

That there is a hunger for these "hi-tech" goods behind the Iron Curtain is unquestioned. Although the Soviet Union is well ahead of the U.S. in conventional military firepower, it is believed to lag behind in its electronic arsenal. To protect this technological edge, the U.S. government has made it illegal to export certain high-technology equipment to the Soviet Bloc and other unfriendly nations without a Commerce Department license. Some equipment is banned altogether from export to those countries.

Breaches in this security wall are coming not only from outright thefts of strategic equipment but also from its diversion through transshipments by seemingly legitimate middlemen and distributors.

At the moment, both the Los Angeles federal grand jury and Santa Clara County sheriff's investigations are focusing on the activities of two international businessmen and onetime partners: Werner Bruchhausen, 41, a German national who now lives in Monte Carlo, and Anatoli Maluta, 46, a Russian-born naturalized U.S. citizen who lives in Torrance, Calif.

Using "Shell" Companies

Search-warrant affidavits filed in state courts in Los Angeles and San Jose earlier this year described Messrs. Bruchhausen and Maluta as "major outlets" for allegedly stolen chips through anywhere from 11 to 50 corporate "shells" they control.

In one recent incident, U.S. Customs agents in Los Angeles seized a missile-guidance system manufactured by Watkins-Johnson Co. of Palo Alto, Calif. and awaiting shipment to the Soviet Union. Details of the seizure were sealed by a federal judge in Los Angeles. But investigators say the military contractor had sold the guidance system to Continental Technology Corp., a company allegedly controlled by Mr. Bruchhausen and Mr. Maluta. Corporation papers show that Continental's officers are Mr. Maluta and two West Germans, the latter described as "associates" of Mr. Bruchhausen, according to law-enforcement sources.

Watkins-Johnson declines all comment on the incident. Mr. Maluta's lawyer says that when he was told that Mr. Bruchhausen had set up the sale to the Soviets through associates in West Germany, his client severed his business relationship with Mr. Bruchhausen. Mr. Bruchhausen couldn't be reached for comment.

Husband and Wife Convicted

Occasionally, producers themselves are involved in violations of the federal ban on shipments to the Soviets. Last December, Spawr Optical Research Inc., a Corona, Calif. company, and its husband and wife owners were convicted by a federal jury in Los Angeles of illegally exporting high-technology laser mirrors, now being tested for use in killer satellites, to the Soviet Union via agents in Germany and Switzerland. The couple earlier had been denied an application to ship the mirrors by the Commerce Department for national security reasons. Their conviction is being appealed.

How strategic merchandise is moved to Russia was well illustrated by the 1979 prosecution of I.I. Industries, a Sunnyvale company, in federal court in San Francisco. The company and its then-owners were convicted of shipping semiconductor-processing equipment to the Soviets without a government license. (I.I. Industries has since been sold to new owners.)

Court records show that the company mislabeled the equipment as goods that didn't need an export license, such as "commercial washing machines" and "industrial ovens." It then shipped the equipment to Canada, which doesn't require a license. From there, the equipment was transshipped to Russia via Switzerland.

In each instance, the middleman was identified as Richard Mueller, a German national. Customs investigators' reports, on file at the agency, identify Mr. Mueller as working for another German, Eugena Schwartz-Nitzska, who is described as having "strong ties" to the Soviet Trade Ministry. Although indicted in the case, Mr. Mueller never returned to the U.S.

Just before the government investigators closed in on the operation, Customs agents sabotaged a final shipment bound for Russia, taking out the electronic equipment and substituting six tons of sandbags, which were duly shipped on to Moscow. What happened when the crates were opened has never been verified, but a Customs agent says, "We never ran into Mueller again."

The search warrants filed in the Bruchhausen-Maluta case by the organized-crime unit of the Santa Clara County sheriff's department provide a detailed overview of the workings of the vast gray market in high-technology electronic materials.

In November 1979, about 10,000 chips (then selling for about $100 each) disappeared from Intel Corp.'s Santa Clara warehouse. They were tiny memory circuits, called "2732s," capable of storing 32,000 bits of data on their fingernail-sized surface. A building block of the rapidly expanding microprocessor technology, 2732s were hotly demanded for all manner of products, from electronic games and Xerox machines to radar-jamming equipment and missile-guidance systems. Customers couldn't get enough of them.

CONTINUED

Suitcase-Size Load

Not much was made of the disappearance of the chips (all 10,000 could have easily fitted into a suitcase) until about a month after their loss. Then a complaint came in from a surprising quarter—Siemens AG, the German electronics giant and a preferred Intel customer. The German firm said that a batch of Intel-brand chips that it had bought—above its normal allocation level and at a suspicious 40% discount—from some European distributors were showing an abnormally high failure rate.

Intel then notified the local sheriff's office of the theft and began to help it in tracing the itinerary traveled by the stolen chips.

From informants, sheriff's deputies learned that the 10,000 unmarked Intel 2732s were stolen prior to completion of in-house testing at Intel. A former Intel reliability technician has been indicted for the theft in state court at Santa Clara. The technician allegedly delivered the stolen chips to John Henry Jackson, a five-time convicted felon, according to court records on file at the Santa Clara court. The technician, now a codefendant in the Intel case, was charged with theft and possession of stolen property, the court documents say.

A Million Counterfeits

According to transcripts of interviews with state and federal agents on file in the Santa Clara court and also in state court in Los Angeles, Mr. Jackson allegedly admitted that he has been trafficking in stolen semiconductors for 14 years. He is quoted as saying that it was "no problem" to steal the Intel parts from shipping docks or storage rooms. Although the circuits weren't stamped with the company's logo, Mr. Jackson allegedly told investigators that he hired a jobber to counterfeit the logo. The jobber is quoted in another court document that "over one million" integrated circuits had been counterfeited for Mr. Jackson over the years. Mr. Jackson couldn't be reached for comment.

Search-warrant affidavits said Mr. Jackson sold a large batch of the stolen 2732s to Mormac Microtechnology Inc. of Tarzana, Calif. An official of Mormac declined comment, on the advice of his lawyer. One of the defendants in the Intel case, charged with grand theft and the possession of stolen property, is Patrick Lyle Ketchum, 26, until recently a Mormac salesman. Federal court records in Los Angeles show that Mr. Ketchum pleaded guilty two years ago to aiding and abetting the use of false information to sell semiconductors. He received probation.

Mr. Ketchum is reputed to have been one of the "money men" of the stolen-chip market, according to a sheriff's department informant quoted in the court affidavits. Mr. Ketchum once allegedly boasted to the informant that he was making $30,000 a month from stolen components, the affidavit says. He lives in a sprawling two-story home on an acre of prime real estate in the exclusive Los Angeles suburb of Hidden Hills. He couldn't be reached for comment and didn't answer messages left at his residence.

More Companies Are Involved

At this point, the names of Messrs. Bruchhausen and Maluta begin to pop up in the network of distributors of stolen parts. According to the affidavit of one informant in the case, "Ketchum and Mormac reportedly deal on a large scale basis with a German and a Russian for whom stolen (integrated circuits) are procured." The document adds Werner Bruchhausen "... a known associate of Patrick Ketchum and Tony Maluta ... is the party to whom Ketchum sells the majority of counterfeit (circuits) he gets from Jackson."

Mr. Maluta's lawyer, Carl A. Capozzola, says his client isn't guilty of any illegal actions and has cooperated fully with the U.S. attorney's office.

The wayward Intel 2732s, meanwhile, passed from Mormac through another company, Space Age Metals of Gardena, Calif. A company spokesman says his company was a victim of the alleged scheme. However, sale documents on file in federal court in Alexandria, Va., indicate the victim sold some $600,000 worth of 2732s to an Arlington, Va., firm, Republic Electronics Corp., which in a 1979 letter to Space Age marveled at "these ever-so-attractive deals."

"What puzzles me," a Republic official wrote, "is that these parts are as rare as hounds' teeth ... I will not question now, why or where. I am not coy nor timid to do this kind of business. I have paid you cash and my customers have paid me cash which seems to cover all the risks." An official at Republic, acknowledging that he knows Mr. Maluta and has done business with Mr. Bruchhausen, denies knowing that the 2732s were stolen and says the company is cooperating with investigators.

Pleading and Pressure

Among Republic's cash-paying customers was a German firm, EBV Elektronik, which in turn supplied Siemens AG with the 2732s for about $6 each, well below the market price.

At this point a snag developed in Intel's attempt to reconstruct the alleged events that occurred after its chips were stolen. Siemens AG apparently resisted attempts to learn the identity of its suppliers. Confidential Intel memorandums, now part of the court record, state that a high Siemens official was "reluctant" to name its supplier out of "concern for the loss of their source of product." After a month of pleading and pressure from Intel, which even considered asking the German courts to confiscate all Siemens products containing the counterfeit chips, the Siemens official finally named EBV.

That official, Gernot Oswald, the director of marketing for Siemens' integrated-circuit division in Munich, remembers the circumstances somewhat differently. "It's absolutely not true (that Siemens was reluctant)," he told a reporter in a telephone interview. "The reason it was cleared up so rapidly is that Siemens was able to help Intel."

Mr. Oswald also told The Wall Street Journal that Siemens had not one but two sources of the stolen 2732s: EBV Elektronik and Werner Bruchhausen himself. He said in the interview that Siemens had bought the 2732s from Mr. Bruchhausen although "we were suspicious from the first moment."

However, Mr. Bruchhausen was "a source to us, a business partner," and "had been supplying the whole industry in Germany with quite a few electronic products," Mr. Oswald says. He acknowledges the gray market as a fact of life in the electronics industry.

A Puzzling Complication

To complicate the intricate gray-market picture further, there's some evidence that U.S. intelligence agents or former agents may be playing a role in the high-tech espionage. Prior to gaining his U.S. citizenship, the Russian-born Mr. Maluta worked for U.S. Air Force intelligence in Germany "performing sensitive duties," law-enforcement sources say. His lawyer confirms that he held a top-secret clearance.

To Silicon Valley lawmen, the involvement of a former U.S. intelligence operative with a man who deals regularly with the Soviet Board of Trade gives the investigation a maddening ambiguity.

"Maluta's a wild card," says Douglas Southard, deputy district attorney for Santa Clara County, who is prosecuting the thefts. "We don't know what he's saying to the federal grand jury. It gets very James Bond-ish. It scares me. I don't get any feedback from the feds at all." Local sheriff's deputies wonder aloud which side Mr. Maluta is really on.

Another intelligence connection clouds the case of I.I. Industries. Edward Breslin, a partner with Mr. Mueller, the German who illegally shipped semiconductor machinery to Russia, had worked 23 years in the U.S. Army Intelligence and the Central Intelligence Agency, according to records in San Francisco federal court. Although Mr. Breslin was the head of a company used by Mr. Mueller to evade U.S. Customs in the I.I. Industries case, he was never charged in the case. Mr. Breslin couldn't be reached for comment.

Semiconductor Thefts Often Go Unreported

By a WALL STREET JOURNAL *Staff Reporter*

SUNNYVALE, Calif. — The government's campaign against technological espionage is often frustrated because semiconductor manufacturers frequently are overly reticent about reporting thefts, lawmen say.

National Semiconductor Corp. and Advanced Micro Devices Inc., for example, initially issued routine denials of any "problem" with thefts to this newspaper, although their components are listed among inventories of items seized in searches of suspected gray-market distributors.

Such lack of candor isn't without reason. "If you report a theft, you could lose your defense contract," says Lt. Robert McDiarmid of the Santa Clara sheriff's department. Moreover, a well-publicized theft tarnishes a company's image and tends to throw customers into the arms of competitors, industry sources say.

George Rakonitz, the security chief for National Semiconductor, concedes, "Management, in general, has a deep interest in suppressing information about crime."

ARTICLE APPEARED ON PAGE 1

CHICAGO TRIBUNE
12 APRIL 1981

Soviet arsenal 'made in U.S.A.'

By James Coates
Chicago Tribune Press Service

WASHINGTON—Through theft, blackmail, and bribery — with an assist from American businessmen eager to make a profit — Soviet agents have obtained enough U.S. high technology to vastly expand their military might — at U.S. expense.

That is the view of many ranking members of the U.S. intelligence community, who say that the Soviet technology-gathering operation is costing American taxpayers billions. Much of the current $189-billion U.S. defense budget is needed to counter Soviet muscle acquired directly through American technology, they add.

Sophisticated U.S. technology is reaching the Soviet armed forces nearly as fast as it is being acquired by U.S. units, say a number of top officials — speaking sometimes on the record and sometimes off.

As a result, Senate Banking Committee Chairman Jake Garn (R., Utah) and others warn, the U.S. must spend billions to counter Soviet military might born of U.S. technology.

THE MOST STARTLING — and dismaying — example to Garn is the discovery that nearly all the engineering breakthroughs in the Soviet SS-18 nuclear missile, which make it accurate enough to imperil all 1,000 American Minuteman ICBM silos in a first strike, are a direct result of buying and stealing U.S. technology.

The SS-18, which carries up to 10 multiple-independently targetable nuclear warheads (MIRVs), is guided by a computer "reverse-engineered" from a sophisticated Hewlett-Packard model stolen by Soviet agents at a 1972 Swiss trade show.

The extremely accurate inertial guidance system — which allows Soviet missile crews to lob their warheads "down the stovepipe" of U.S. siloes — is made possible by American ballbearing technology. Soviet engineers now use machines called Centalign B, bought from a New England firm under a Department of Commerce license, to grind bearings with a degree of precision offered by no other machine. The license was granted despite intelligence community warnings.

A military analyst disclosed that the SS-18 guidance systems use an on-board laser measuring device acquired in California by a KGB (Soviet intelligence) operation coordinated out of the Soviet trade consulate in San Francisco.

DR. MILES COSTICK, president of the Institute on Strategic Trade here and a frequent debriefer of Iron Curtain defectors, said Russian engineers have told him in interviews that they observed bearings from the Centalign B machines being installed in the SS-18s.

In a 1980 report to the Banking Committee, Garn called the sale of the precision grinders "ill advised" and noted: "The first immediate effect of increased Soviet MIRV accuracy on the American people is the need to build and deploy the MX ICBM, which will cost over $30 billion in constant (1980) dollars."

Since then the Congressional Budget Office has estimated that the MX missile will cost $40 billion.

The SS-18 appears to be the costliest loss to U.S. interests, but it is far from the only case in which an ambitious and often illegal KGB operation has sapped American companies, scientists, and businessmen of technology far more sophisticated than what is available inside the Soviet bloc.

Some other examples:

● Commerce Department investigators found that the GEO Space Corp. of Houston exported seismographic equipment used for exploration of underground oil and gas to the Soviets without obtaining proper licenses. The computerized sensing equipment was adapted by the Soviets for use aboard Russian naval vessels, where it can detect a U.S. submarine as easily as it can a Texas gas deposit.

Walter and Frances Spawr, a couple who operated a Corona, Cal., optical research company, were indicted late last year for deliberately exporting sophisticated copper-plated, water-cooled laser mirrors to the Soviets. A high Commerce Department source said in an interview that the CIA has found that the laser mirrors are being tested in the Soviet hunter-killer satellite program.

● In August FBI agents posing as Soviet officials arrested Marc Andre DeGeyter of Alexandria, Va., as he tried to sell computer tapes produced by American defense contractors for $500,000. The tapes contained the design for building a "super chip" technology that could be used to inventory an entire army or guide terrain-hugging Cruise missiles over Soviet territory.

Federal agents found a $450,000 letter of credit in DeGeyter's briefcase guaranteed by Techmashimport, a Soviet state trading company, law enforcement sources said.

U.S. officials have concluded that in the last 18 months the Soviets have gained the capacity to build microcomputer chips such as those made in California's "Silicon Valley," south of San Francisco, which has become the world's leading research and development center for solid state electronics. The machines to build the components were shipped to Russia by an American company, L.I. Industries, in boxes labeled "air-conditioners" and "washing machines."

Experts who discussed the technology drain in interviews told of a decade-long

CONTINUED

For years, American know-how and equipment have contributed to Soviet military might. This is the first of a three-part series examing how the Russian military has taken advantage of U.S. technology.

spy war in which Western intelligence operatives have sparred with their Soviet KGB and GRU (military intelligence) counterparts from the board rooms of Silicon Valley to the back alleys of Hong Kong.

"One thing I'd have to say," said Francis W. "Bud" Mullen, deputy FBI Director, "is that a lot of the things we accomplish are things you will never hear about: transactions that never occurred because we stopped them.

"I think you will appreciate, that often it is not in the (American) national interest to broadcast what we know about what they (the KGB) are doing."

COSTICK, WHO operates under fewer restraints than Mullen, told in a recent report of a dramatic KGB operation in which the KGB attempted to buy a bank in an apparent effort to obtain damaging data to blackmail Silicon Valley scientists.

In this case a man calling himself Amos Dawe approached officials of the Peninsula National Bank in Burlingame, south of San Francisco, in the early 1970s with an offer to buy the bank.

Costick said that Dawe presented letters of credit worth $70 million as part of his offer. The credit was found to be guaranteed through the Moscow Narodny Bank.

The CIA discovered that Dawe was really Law Sheng Moh from Hong Kong. British intelligence apparently supplied information about Dawe to a financial news publication, "Target," and a state banking investigation was launched. The deal collapsed.

"MY INFORMATION is that Law Sheng Moh was trying to buy at least two other California banks because bank owners can get detailed information about people who can become extortion targets," Costick said.

At the Commerce Department, where officials have established a net of informants from the business community, underworld, the CIA, Interpol, and other intelligence-gathering organizations, a key executive noted a "dramatic upswing in KGB activity" in the last year.

"We have cases in every port you can imagine," said the official, who asked not to be identified. "About 50 per cent of our cases move through New York and about 25 per cent are in California. Chicago is another place where we keep busy."

He said that the case involving Spawr Optical Research, Inc., of California may be the most damaging example of the KGB operation recorded recently.

INTERNAL COMMERCE Department and CIA studies have concluded that the Soviets can use the Spawr laser mirrors to burn holes in U.S. spy and early warning satellites.

Soviet engineers apparently are studying the possibility of placing the Spawr mirrors in one satellite orbiting just below the targeted U.S. satellite while a second Soviet satellite orbits above the target.

A laser beam would then be generated between the two Soviet craft by the mirrors and deflected to strike the American satellite as it passed.

This official noted that although the criminal penalties imposed in the Spawr case and in similar cases appear light, Commerce Department investigators are "encouraged" because Walter Spawr received a 10-year jail term. "Even though all but six months was suspended for Spawr, the verdict was still important to us," the officials said.

Longtime trade partners now global adversaries

THE UNITED States and Russia have been trading partners throughout this century, even before the 1917 Bolshevik Revolution. A 1980 Senate study noted, for example, that in 1914 Singer Sewing Machine Co. had holdings worth more than $100,000 in Russia.

As part of the 1928-33 Soviet "five Year Plan," the Arthur G. McGee Co. of Cleveland helped build a large steel plant in Magnitogorsk, USSR. The mill was a duplicate of the United States Steel Corp. Gary Works, according to a Senate Permanent Investigations Subcommittee report.

Since the U.S.-Soviet trade agreement signed by President Richard Nixon in October, 1972, exchanges have increased, and many intelligence analysts have warned that the Soviets are building their military machine with technology acquired in trade.

IN 1978 THE Soviets bought $2.8 billion worth of U.S. goods, mainly larg scale grain purchases, according to Department of Comverce figures. That amount is roughly one-third of the trade in 1978 between the U.S. and Taiwan.

In 1979, U.S. goods sold to the Soviets were valued at $1.7 billion; in 1980, after the Carter administration embargo imposed in response to the Soviet invasion of Afghanistan, sales plummeted to $857 million, Commerce Department figures show.

In an effort to prevent damage to national security by sales of high technology, the U.S. established a licensing procedure that bans certain exports and regulates others.

In 1980, according to Commerce Department reports, licenses for items valued at $736 million were approved for export to the USSR, Eastern Europe, the Mongolian Peoples Republic, and Communist China.

ARTICLE APPEARED ON PAGE 1

CHICAGO TRIBUNE
13 April 1981

Soviets walk right in, take American technology home

For years, American know-how and equipment have contributed to Soviet military might. This is the second article of a three-part series examining how the Russian military has taken advantage of U.S. technology.

By James Coates
Chicago Tribune Press Service

WASHINGTON — The 40 Soviet aircraft specialists had a U.S. Department of State letter of introduction when they visited factories of Boeing, Lockheed, and McDonnell Douglas for a 1973 tour of production lines and shop talk.

They watched Americans building the new wide-body jets — the 747 at Boeing, the DC-10 at McDonnell Douglas, and the L-1011 at Lockheed. Last year the CIA learned while debriefing a defector that the Soviet visitors wore special shoes that picked up metal scraps from the factory floors.

The shavings were analyzed in Moscow and that enabled the Russians to acquire the metal alloys needed to produce their giant Ilyushin II-76T troop transport planes, according to congressional sources who have received CIA briefings on the matter.

Such field trips are just part of an ambitious overt and covert Soviet program that each year obtains some of the most sophisticated technology being developed by the United States.

THE TECHNOLOGY is being used to bolster Soviet military might, and congressional, administration, and private experts say the U.S. must increase military spending to counter Soviet advances.

Among the examples of how the Soviets acquire the latest American know-how at a fraction of what it costs the U.S.:

● Each year a new batch of highly trained Soviet scientists, usually 35 or older, become "exchange students" and enrolls in top American universities to study high technology subjects. Dismayed U.S. experts note that, by contrast, nearly every American in the exchange program studies "soft" cultural and historical topics, such as Soviet fairy tales and Russian chamber music.

● The Russian Embassy here spends several million dollars a year on a standing order for copies of each of the 80,000 technical reports deposited at the Department of Commerce's National Technical Information Service.

● Hundreds of times a year, Soviet businessmen negotiate with high technology American companies, ostensibly offering deals in which the U.S. may sell products in the U.S.S.R. once the Americans obtain required export licenses. Actually, such experts as FBI Director William Webster warn, the Soviets use the bargaining sessions to acquire confidential business processes. Commerce Department spokesmen said that the license applications shown to Soviets are kept secret from the public because they often contain confidential information.

Vasili I. Khlopyanov and Vladimir Alexandrov, two KGB executives at the Soviet trade consulate in San Francisco, have been observed operating a program to obtain products and know-how being produced in California's so-called Silicon Valley, according to U.S. intelligence sources. That is a major technology area. More than a dozen major diversions of the highest computer technology have been traced to the Soviet bloc from this operation. The KGB is the Soviet Secret Police.

Webster recently told a group of California businessmen, "I think you would be astonished by the voraciousness of the appetites of hostile intelligence gatherers."

Webster has issued similar warnings in speeches in Chicago, New York, and St. Louis. He told the Californians, "Hostile intelligence gatherers have a strong interest in technological secrets, especially about computers, micro-electronics, fiber optics, and lasers.

He said 11,000 American companies handle classified information through government contracts. The Soviets have obtained much of that data simply by negotiating with U.S. businessmen, he said.

ACCORDING TO FBI reports, as many as 2,000 of the FBI's 7,800 agents in the U.S. work in counterintelligence full time to keep track of the thousands of visitors from the U.S.S.R. and Soviet bloc countries.

John Morrison, a spokesman for Webster, acknowledged that the bureau almost never makes an arrest in the technology transfer area.

"We've had maybe one case in five or six years" with arrests, Morrison said. He cited the arrest last year of Marc Andre DeGeyter, who allegedly tried to sell sensitive computer programs to an undercover agent.

A leading analyst of the Soviet effort to acquire American technology is Dr. Miles Costick, president of the Institute on Strategic Trade here and a close associate of several top intelligence advisers in the Reagan administration.

Costick has estimated that the Soviets have obtained technical equipment and processes that would have cost them more than $100 billion to get without U.S. aid.

Considered particularly significant is Costick's analysis of how the Soviets produced their current generation of ballistics missiles by patiently working through the American system to obtain key technology.

MUCH OF THE technology that went into the Soviet missiles came from universities in the Boston area and District of Columbia, Costick said. He cited the case of Anatoly Kochev as one of the more blatant examples. Costick, who gets much of his information debriefing Soviet bloc defectors, said that in the late 1960s, Kochev was assigned to the Leningrad Polytechnical Institute to build a device called an accelerometer.

It measures changes in the pull of gravity on an airborne vehicle and is crucial to accurate flight for a guided

CONTINUED

ARTICLE APPEARED ON PAGE 1

CHICAGO TRIBUNE
13 April 1981

Soviets walk right in, take American technology home

For years, American know-how and equipment have contributed to Soviet military might. This is the second article of a three-part series examining how the Russian military has taken advantage of U.S. technology.

By James Coates
Chicago Tribune Press Service

WASHINGTON — The 40 Soviet aircraft specialists had a U.S. Department of State letter of introduction when they visited factories of Boeing, Lockheed, and McDonnell Douglas for a 1973 tour of production lines and shop talk.

They watched Americans building the new wide-body jets — the 747 at Boeing, the DC-10 at McDonnell Douglas, and the L-1011 at Lockheed. Last year the CIA learned while debriefing a defector that the Soviet visitors wore special shoes that picked up metal scraps from the factory floors.

The shavings were analyzed in Moscow and that enabled the Russians to acquire the metal alloys needed to produce their giant Ilyushin Il-76T troop transport planes, according to congressional sources who have received CIA briefings on the matter.

Such field trips are just part of an ambitious overt and covert Soviet program that each year obtains some of the most sophisticated technology being developed by the United States.

THE TECHNOLOGY is being used to bolster Soviet military might, and congressional, administration, and private experts say the U.S. must increase military spending to counter Soviet advances.

Among the examples of how the Soviets acquire the latest American know-how at a fraction of what it costs the U.S.:

● Each year a new batch of highly trained Soviet scientists, usually 35 or older, become "exchange students" and enrolls in top American universities to study high technology subjects. Dismayed U.S. experts note that, by contrast, nearly every American in the exchange program studies "soft" cultural and historical topics, such as Soviet fairy tales and Russian chamber music.

● The Russian Embassy here spends several million dollars a year on a standing order for copies of each of the 80,000 technical reports deposited at the Department of Commerce's National Technical Information Service.

● Hundreds of times a year Soviet businessmen negotiate with high technology American companies, ostensibly offering deals in which the U.S. may sell products in the U.S.S.R. once the Americans obtain required export licenses. Actually, such experts as FBI Director William Webster warn, the Soviets use the bargaining sessions to acquire confidential business processes. Commerce Department spokesmen said that the license applications shown to Soviets are kept secret from the public because they often contain confidential information.

Vasili I. Khlopyanov and Vladimir Alexandrov, two KGB executives at the Soviet trade consulate in San Francisco, have been observed operating a program to obtain products and know-how being produced in California's so-called Silicon Valley, according to U.S. intelligence sources. That is a major technology area. More than a dozen major diversions of the highest computer technology have been traced to the Soviet bloc from this operation. The KGB is the Soviet Secret Police.

Webster recently told a group of California businessmen, "I think you would be astonished by the voraciousness of the appetites of hostile intelligence gatherers."

Webster has issued similar warnings in speeches in Chicago, New York, and St. Louis. He told the Californians, "Hostile intelligence gatherers have a strong interest in technological secrets, especially about computers, micro-electronics, fiber optics, and lasers.

He said 11,000 American companies handle classified information through government contracts. The Soviets have obtained much of that data simply by negotiating with U.S. businessmen, he said.

ACCORDING TO FBI reports, as many as 2,000 of the FBI's 7,800 agents in the U.S. work in counterintelligence full time to keep track of the thousands of visitors from the U.S.S.R. and Soviet bloc countries.

John Morrison, a spokesman for Webster, acknowledged that the bureau almost never makes an arrest in the technology transfer area.

"We've had maybe one case in five or six years" with arrests, Morrison said. He cited the arrest last year of Marc Andre DeGeyter, who allegedly tried to sell sensitive computer programs to an undercover agent.

A leading analyst of the Soviet effort to acquire American technology is Dr. Miles Costick, president of the Institute on Strategic Trade here and a close associate of several top intelligence advisers in the Reagan administration.

Costick has estimated that the Soviets have obtained technical equipment and processes that would have cost them more than $100 billion to get without U.S. aid.

Considered particularly significant is Costick's analysis of how the Soviets produced their current generation of ballistics missiles by patiently working through the American system to obtain key technology.

MUCH OF THE technology that went into the Soviet missiles came from universities in the Boston area and District of Columbia, Costick said. He cited the case of Anatoly Kochev as one of the more blatant examples. Costick, who gets much of his information debriefing Soviet bloc defectors, said that in the late 1960s, Kochev was assigned to the Leningrad Polytechnical Institute to build a device called an accelerometer.

It measures changes in the pull of gravity on an airborne vehicle and is crucial to accurate flight for a guided

CONTINUED

missile. Kochev was in charge of the accelerometer project for the Soviet missile program at the time he was sent as an exchange student to Catholic University here to study accelerometer construction.

Shortly after his return to the U.S.S.R., there was a dramatic increase in Soviet missile accuracy. Soon after that, the Soviet Union successfully fired a multiple-warhead missile. Costick indicated that defectors have told him that the first missile breakthrough came from Kochev's studies in the U.S.

There are indications that the Soviet drive to acquire U.S. high technology is moving away from the already successful missile project to focus on the American missile-carrying Trident submarine fleet, which still poses a major threat to adversaries.

The big breakthrough for the Soviets in that area has been the acquisition of tiny electronic devices called array transform processors from a Texas oil exploration firm.

These components, called APs, allow a computer to interpret almost instantly millions of tiny variations in sounds being bounced off deeply buried geologic formations when explosives are detonated.

After the devices were acquired, through GEO Space Corp. of Houston, it was discovered that the Soviets were using them for computers to find American submarines by analyzing tiny variations in sonar signals, not for geological exploration.

Costick told a Senate committee: "I have interviewed for two days a former Soviet intelligence specialist, a geologist by profession, who revealed to me that he and Soviet Navy personnel — trained in Houston — had carried on board Soviet submarines . . . APs and installed them there next to the shipboard computers."

Tuesday: How Soviets use the American system.

CHICAGO TRIBUNE
14 April 1981

U.S. acts tardily to halt Soviet siphoning of technology

By James Coates
Chicago Tribune Press Service

WASHINGTON — At least twice last year United States officials moved only at the last minute to halt the shipment of military factory equipment to the Soviet Union, despite White House orders to cut off all such transactions.

On March 28, 1980, Commerce Secretary Philip Klutznick sent customs agents from here to New York to embargo crates of aviation machinery. Experts had found that the equipment would cut at least in half the overhaul time period for Soviet helicopters, MIG jets, and Tupolev bombers in Afghanistan and elsewhere.

New York customs officials had refused to stop the shipment, and the crates were on pallets awaiting shipment when the agents arrived from here, according to a report presented in 1980 to the Senate Governmental Affairs Committee by Sen. Jake Garn (R., Utah).

On May 6, 1980, 4½ months after Soviet units swarmed over the Afghanistan frontier in trucks built in the American-designed and supplied Kama River plant, in Russia, Pentagon agents finally forced the bureaucracy to halt the shipment of a 200-foot-long diesel engine assembly line, which would have doubled the factory's capacity.

Experts studying the steady drain of American technology to the Soviets through purchases, theft, bribery and sometimes simply copying from voluminous American public records note that these two cases are considered successful in that the transfer was stopped.

For years, American know-how and equipment have contributed to Soviet military might. This is the final article in a three-part series examining how the Russian military has taken advantage of U.S. technology.

HUNDREDS OR PERHAPS thousands of other times, U.S. technology has been passed to the U.S.S.R. at bargain-basement rates. Some experts have computed that it would have cost Moscow roughly $100 billion more to acquire its current level of technological expertise if it had not obtained it from the West.

As a result, Garn and other experts said, American taxpayers are confronted with a staggering U.S. defense budget of $189 billion this year and more next year — much of it needed to combat Soviet military prowess acquired directly from U.S. sources.

American intelligence organizations have traced Soviet acquisitions — from the Ryad I, Ryad II, and Ryad III computers which are virtual copies of the IBM 360, 370 and E Series, to the Strella battlefield missile, a copy of the U.S. Red Eye weapon.

FROM THE ROLLS-Royce engines powering Soviet troop transports to the mills dating from the 1930s, designed by United States Steel Corp., Western know-how is noted everywhere in the Soviet military machine.

Russian tanks captured in the 1973 Mideast war were found to be using periscopes and other equipment manufactured in the U.S., a Senate committee was told recently by Pentagon officials.

The Soviet's ZIL plant uses U.S.-made equipment, which is operated by teams of American workers. There the Soviets produce several types of vehicles, including the Red Army missile launchers that U.S. spy satellites photographed in Afghanistan.

Soviet and Warsaw bloc defectors have told American debriefing officers of numerous instances in which the military establishment directly acquired high technology hardware that Russian negotiators insisted they wanted for peaceful uses.

Soviet dissident Anatoly Shcharansky was charged in a Russian court with illegally telling Western journalists that his country had violated U.S. Department of Commerce agreements by using American computers in its military programs.

EACH YEAR 1,000 Soviet businessmen and roughly 6,000 visitors from Eastern Europe companies fan out across the U.S. to visit corporate officers and discuss acquiring technological items under U.S. Commerce Department license.

FBI Director William Webster has warned businessmen to be wary, because often these business "deals" are simply a ruse to visit factories and obtain information through conversations.

Such aggressive information gathering is not a Soviet practice alone. U.S. officials in the Soviet Union make similar efforts. A top Navy source told, for example, of the time U.S. Vice Adm. Hyman Rickover had his engineers design a tiny radiation sensor inside a fountain pen so he could carry it aboard a Soviet vessel on a ceremonial visit and ferret out reactor secrets.

CONTINUED

2

But intelligence community experts complain that it is much easier for Soviet operatives to glean information in the open U.S. society than for Americans to work in the U.S.S.R. and Eastern bloc, where no such freedom is allowed.

IN TESTIMONY before the Senate Governmental Affairs Committee, Commerce Department officials outlined ways that Soviet businessmen elicit useful data simply by working within the American system.

One of the more effective ways is to approach several competing U.S. firms and to ask them to obtain a license from the Commerce Department for exports to the Soviet Union. The license applications, which are shared with the Soviets but kept from U.S. public view, often contain key data about the process being sought, according to testimony by Eric Hirschorn, a former export chief at the agency.

Another way to obtain information is to apply for a patent. The U.S. government will then make a search of other patents and report to the applicant certain details of any industrial process similar to the one he wants to patent, Hirschorn said.

OFTEN, AS IN the case of the aborted March, 1980, shipment of aircraft machinery, the free enterprise system and federal bureaucracy become Soviet allies in the technology drain.

In that case, Sermetel, Inc., a company in Limerick, Pa., signed a contract to export to the Soviet Union a patented ceramic-metallic (CERMET) oxide treatment process for the moving parts of jet turbines. The sale meant millions to the company and it was approved and licensed by the Commerce Department.

Concerned Department of Defense officials objected that the sale would give the Soviets not only machines to treat their planes for a couple of years, as originally intended, but also the capability of creating the crucial process themselves.

The CERMET process coats the machines with a preservative so tough that engine parts last several times longer and overhaul time is "greatly reduced," according to a report on the sale written by Sen. Garn.

WHILE PENTAGON and Commerce Department officials argued over national security, Sermetel crated its equipment and sent it to New York for shipment to the Soviet Union.

It took a phone call from Zbigniew Brzezinski, U.S. national security adviser, to Commerce Secretary Klutznick, to stop the shipment, Sen. Garn recalled.

The CERMET affair shows, according to Garn, that even when the U.S. tries to stop the technology drain to the Soviet Union, there can be considerable difficulty.

Because the U.S. is an open society and because efforts to stop technology acquisition by Soviets often hurt businesses such as Sermetel, there are many pressures not to block these deals, even when they prove controversial, Commerce Department officials acknowledge.

GARN AND OTHER Senate leaders are sponsoring legislatin to establish an independent Office of Strategic Trade, without ties to the Commerce Department.

The department, which was created to encourage business, should not have control over the sensitive transactions between the U.S. and the Soviet Union, proponents argue.

Lawrence J. Brady, who directed the export office at the Commerce Department in the Carter administration, resigned last year after publicly complaining about the drain and questioning the administration's motives.

He became a key adviser to the Reagan transition team and is now a consultant to his former Commerce Department office. He is favored, several congressional sources acknowledged, to head the strategic trade office, if one is set up.

Brady told the Senate committee last year: "Administrators must recognize that we are engaged in strategic confrontation with the Soviet Union and that right now the Soviets are winning in their strategy of lull and divide against the Western economies, while it is engaged at the same time in a resource war of economic attrition against the West."

ARTICLE APPEARED ON PAGE A-3
THE WASHINGTON POST
4 April 1981

Russian Cloak-and-Briber Goal: American High-Technology Secrets

By Thomas O'Toole
Washington Post Staff Writer

When the Spawr Optical Research Co. of Corona, Calif., applied for a license to export 10 laser mirrors to the Soviet Union four years ago, the application was turned down by the U.S. government because the lasers and copper mirrors could be used as anti-satellite weapons in space.

Rejection of his application didn't stop Walter Spawr, president of Spawr Optical, from shipping about 50 laser mirrors to a laser research laboratory in Moscow.

Testimony in U.S. District Court in Los Angeles last year showed that Spawr deliberately understated the value of his high-energy laser mirrors to the Customs Service, and then shipped the mirrors to firms in Switzerland and West Germany, which he said was their final destination.

In Switzerland and Germany, a West German named Wolfgang Weber, who was a business associate of Spawr, reconsigned the mirrors to Moscow.

Intelligence sources told the court in Los Angeles that the mirrors already may have been used in tests of Soviet anti-satellite weapons, where lasers were used to burn holes in aircraft to blow them up.

Spawr was convicted of violating the Export Administration Act and given a 10-year suspended sentence on condition he serve six months in jail. His company was fined $100,000.

The Spawr case spotlights a steadily rising effort by the Soviet Union to pry away the secrets of American high technology by means they rarely used in the Cold War years of the '50s and '60s.

The Soviets, offering huge sums of money for lasers, fiber optics and computers, bribing company officials and using European middlemen and dummy Polish, Hungarian and Romanian corporations, are conducting an unprecedented assault on the industries of America.

"The Russian targets are no longer weapons and strategy," FBI Director William H. Webster told The Washington Post. "The emphasis is now on technology, and they will go to any lengths to get it."

Lasers have military uses in space; fiber optics can be used to make small, secret communications devices. Computers have thousands of military and intelligence applications.

The FBI says at least 1,000 of the 2,800 Soviet and East European diplomats in the United States are "known or suspected" intelligence officers whose assignment is at least in part the acquisition of high technology.

Also, 2,500 Soviet engineers and scientists visit this country every year on trade missions, which may be another way of saying that at least some of them are here to steal industrial secrets.

At no time in its history has the FBI had a larger, more active counterintelligence operation. Of the 7,800 agents in its 59 field offices, as many as 2,000 are engaged full-time in counterintelligence.

Their task isn't easy, mostly because it's corporate and not Pentagon secrets the Soviets are after. In California's high-technology Silicon Valley, more than 500 companies have access to classified information. Nationwide, 11,000 companies have the same access.

At least five times, the Soviets have been able to bribe American company officials to assist them in buying instruments on the export control list. Swiss and German middlemen also have been bribed by the Soviets to buy controlled American devices.

Usually, sheer greed is involved. Says a federal official: "We haven't come across a case yet that involved ideological espionage. The sales to the Russians have always been for money."

The top Soviet targets are microelectronics and computers. Last year, a Belgian, Marc Andre DeGeyter, offered a $500,000 bribe to an official of Software A.G. in Reston, Va., to steal a coded computer program for the Soviets. The program would allow the Russians instant inventory control at any military base, no matter how large or complex. DeGeyter got a four-month jail sentence.

DeGeyter's case was unusual because he was caught before anything found its way into Soviet hands.

Two years ago, two top officials of I.I. Industries in San Jose, Calif., were found guilty of violating the same law after federal agents discovered they had shipped more than $1 million in computer machinery to the Soviet Union without a license by selling it to a West German businessman, who forwarded it to Moscow.

The first shipment was through a phantom company in Montreal, which sent it to Zurich and then Moscow. The next three shipments went to a fictitious company in Kansas City, where the computer machinery was crated with air conditioners and washing machines and sent through Germany and The Netherlands to Moscow.

Almost as high as computers on the Soviet want list are lasers and fiber optics. Laser and fiber optics parts have been carried out of the United States in East European diplomatic pouches. The FBI has investigated at least 30 cases in which the Soviets offered bribes to buy lasers and fiber optics that were on the export control list.

Federal agents often learn of illegal technology exports while they are in progress. A favorite federal tactic is to intercept an illegal shipment and substitute something meaningless. At least twice, federal agents packed computer machinery boxes with sand that was then transshipped to Europe on its way to Moscow.

So heavy is the traffic between the United States and the Soviet Union that the Commerce Department, which administers the export control law, is now in the counterintelligence business.

CONTINUED

Not only does staid old Commerce have its own agents, but it also has a stable of informers whom it sometimes pays out of its own informer fund. Who are its informers? People in the export business, people working at air freight companies, people working on the docks in New York and San Francisco.

"It's hard to say these cases are on the increase, but in 1980 we closed twice as many cases as we closed the previous year," said Sharon Connolly, director of the enforcement division of the Commerce Department's Office of Export Administration. "If these cases are not on the increase, we're certainly hearing more about them."